

Amendments to the Claims

1. (currently amended) A security processing method comprising:

receiving, by a security processor, an internal outbound packet ~~packets~~
from a ~~Gigabit~~ an Ethernet controller network, wherein the internal outbound packet
includes a flow identifier for the packet and a security processor identifier;

processing at least a portion of the received packet ~~packets~~ if the
security processor identifier matches an identifier associated with the security
processor, wherein the processing includes: the processing consisting of at least one
of the group of encrypting, decrypting and authenticating

using the flow identifier as a direct address handle to retrieve a
security association for the received packet,

performing a cryptographic operation on a portion of the received
packet using at least a portion of the retrieved security association, and

assembling an outbound network packet including a header and the
cryptographically processed portion of the received packet; and

transmitting, from the security processor, the outbound network packet
~~at least one result of the processing of the at least a portion of the received packets.~~

2. (currently amended) The method of claim 1 wherein ~~processing~~
performing the cryptographic operation comprises performing one or more IPsec
operations.

3. (original) The method of claim 2 wherein the IPsec operations comprise
adding or removing protocol elements.

4-6. (canceled)

7. (currently amended) The method of claim 1 wherein the security processor resides on a network interface card (NIC) comprises an integrated circuit.

8. (currently amended) A security processor comprising:

at least one Gigabit media access controller (MAC) MAC; and

at least one processor configured to: [[,]] ~~connected to send data to and receive data from the at least one Gigabit MAC, for encrypting, decrypting or authenticating at least a portion of the data~~

receive an internal outbound packet from an Ethernet controller via the MAC, wherein the internal outbound packet includes a flow identifier for the packet and a security processor identifier,

process at least a portion of the received packet if the security processor identifier matches an identifier associated with the security processor, including:

using the flow identifier as a direct address handle to retrieve a security association for the received packet,

performing a cryptographic operation on a portion of the received packet using at least a portion of the retrieved security association, and

assembling an outbound network packet including a header and the cryptographically processed portion of the received packet.

9. (original) The security processor of claim 8 wherein the at least one processor comprises at least one IPsec processor.

10. (currently amended) The security processor of claim 9 wherein the IPsec processor is configured to add ~~adds~~ IPsec protocol elements to or to remove ~~removes~~ IPsec protocol elements from the data.

11. (canceled).

12. (currently amended) The security processor of claim 8 further comprising at least one data memory for storing security association information for use by the at least one processor , wherein the security association information includes a handle and security association data.

13 - 14 (canceled).

15. (currently amended) The security processor of claim 8 wherein the security processor resides on a network interface card (NIC) ~~is an integrated circuit.~~

16. (currently amended) An in-line security processor comprising:
a plurality of ~~Gigabit~~ media access controllers (MACs) ~~MACs~~; and
at least one processor configured to [[,]] ~~connected to receive data from at least one of the Gigabit MACs and to send data to at least one of the Gigabit MACs, for encrypting, decrypting or authenticating at least a portion of the data~~
receive an internal outbound packet from an Ethernet controller via at least one of the plurality of MACs, wherein the internal outbound packet includes a flow identifier for the packet and a security processor identifier,
process at least a portion of the received packet if the security processor identifier matches an identifier associated with the security processor,
including:

using the flow identifier as a direct address handle to retrieve a security association for the received packet,
performing a cryptographic operation on a portion of the received packet using at least a portion of the retrieved security association, and
assembling an outbound network packet including a header and the cryptographically processed portion of the received packet.

17. (original) The in-line security processor of claim 16 wherein the at least one processor comprises at least one IPsec processor.

18. (currently amended) The in-line security processor of claim 17 wherein the IPsec processor is configured to add ~~adds~~ IPsec protocol elements to or to remove ~~removes~~ IPsec protocol elements from the data.

19. (canceled).

20. (original) The in-line security processor of claim 16 further comprising at least one data memory for storing security association information for use by the at least one processor.

21. (currently amended) A security processing system comprising:

at least one media access controller (MAC);

at least one security processor configured to:

receive an internal outbound packet from an Ethernet controller via at least one MAC, wherein the internal outbound packet includes a flow identifier for the packet and a security processor identifier,

process at least a portion of the received packet if the security processor identifier matches an identifier associated with the security processor, including:

using the flow identifier as a direct address handle to retrieve a security association for the received packet,

performing a cryptographic operation on a portion of the received packet using at least a portion of the retrieved security association, and

assembling an outbound network packet including a header and the cryptographically processed portion of the received packet; and

at least one switch for distributing or collecting packets between the at least one media access controller and the at least one security processor.

22. (original) The security processing system of claim 21 wherein the at least one media access controller comprises at least one Gigabit MAC.

23. (currently amended) The security processing system of claim 21 ~~further comprising wherein the~~ at least one security processor ~~for allocating is further configured to allocate~~ memory space associated with security associations used by the at least one security processor.

24. (original) The security processing system of claim 21 wherein the at least one switch associates VLAN tags with the at least one media access controller.

25-26. (canceled)

27. (currently amended) A chassis-based switch comprising:

at least one backplane;

at least one processing blade connected to the at least one backplane,
the at least one processing blade comprising at least one media access controller; and
at least one switching blade connected to the at least one backplane,
the at least one switching blade comprising:

at least one security processor configured to:

receive an internal outbound packet from an Ethernet
controller, wherein the internal outbound packet includes a flow identifier for the
packet and a security processor identifier,

process at least a portion of the received packet if the security
processor identifier matches an identifier associated with the security processor,
including:

using the flow identifier as a direct address handle to
retrieve a security association for the received packet,

performing a cryptographic operation on a portion of the
received packet using at least a portion of the retrieved security association, and

assembling an outbound network packet including a header
and the cryptographically processed portion of the received packet; and

at least one switch for routing packets between the at least one
media access controller and the at least one security processor.

28 -32. (canceled)

33. (currently amended) A security processing system comprising:

at least one Ethernet configured to controller for:

~~executing TCP operations~~ receive a TCP/IP packet in a data flow
and ~~storing~~ store context information associated with the TCP/IP packet TCP
operations;

identify flow identification information for the data flow including
a flow identifier ~~generating information associated with at least one security~~
~~association from the context information;~~ and

generate ~~generating at least one~~ an internal packet including a
security identifier header having the flow identifier, a security processor identifier,
and at least a portion of the TCP/IP packet ~~the information associated with at least one~~
~~security association;~~ and

at least one security processor, connected to receive the internal ~~at least~~
~~one packet from the at least one Ethernet controller, the at least one security processor~~
configured to for:

receive the internal packet from an Ethernet controller, wherein the
internal outbound packet includes a flow identifier for the packet and a security
processor identifier,

process at least a portion of the received packet if the security
processor identifier matches an identifier associated with the security processor,
including:

using the flow identifier as a direct address handle to retrieve a
security association for the received packet,

performing a cryptographic operation on a portion of the
received packet using at least a portion of the retrieved security association, and

assembling an outbound network packet including a header and the cryptographically processed portion of the received packet.

~~locating the at least one security association using the information associated with at least one security association; and~~

~~encrypting, decrypting or authenticating data using the security association.~~

34. (withdrawn) A method of configuring a security processor comprising:
generating configuration information;

formatting the configuration information into at least one packet; and

sending the at least one packet over a Gigabit Ethernet network to a security processor.

35. (withdrawn) The method of claim 34 wherein the at least one packet comprises at least one IPsec packet.

36. (withdrawn) A method of configuring a security processor comprising:

receiving at least one packet containing configuration information over a Gigabit Ethernet network;

extracting the configuration information from the at least one packet; and

configuring a security processor using the extracted configuration information.

37. (withdrawn) The method of claim 36 wherein the at least one packet comprises at least one IPsec packet.

38. (withdrawn) A method of configuring a security processor comprising:

- generating at least one security association;
- formatting the at least one security association into at least one packet; and
- sending the at least one packet over a Gigabit Ethernet network to a security processor.

39. (withdrawn) A method of configuring a security processor comprising:

- receiving at least one packet containing at least one security association over a Gigabit Ethernet network; extracting the at least one security association from the at least one packet; and
- storing the extracted at least one security association.

40. (original) A method , in a Ethernet controller, of generating an internal packet for transmission to a security processor over a PCI bus ~~a TCP frame~~ comprising:

- receiving a TCP/IP packet in a data flow and storing context information associated with the TCP/IP packet;

- identifying flow identification information for the data flow including a flow identifier;

- generating the internal packet including a security identifier header having the flow identifier, a security processor identifier, and at least a portion of the TCP/IP packet; and

- transmitting the internal packet to the security processor over the PCI bus for cryptographic processing

~~generating at least one header comprising an Ethernet header and a reference to an address of a security association; and appending the at least one header to an original TCP frame.~~

41 -50. (canceled).

51. (currently amended) The security processing system of claim 33 [[49]] wherein the at least one security processor is further configured to modify ~~modifies~~ at least one checksum in the at least one security header added by the at least one network controller.

52. (currently amended) The security processing system of claim 33 [[47]] wherein the at least one ~~network~~ Ethernet controller modifies at least one maximum transmitted unit size in accordance with modifications the security processor makes to at least a portion of the packets.

53. (currently amended) The security processing system of claim 33 [[47]] wherein the at least one ~~network~~ Ethernet controller reduces at least one TCP/IP payload size in accordance with at least one security header and trailer size added to at least a portion of the packets.

54 - 55 (canceled).

56. (currently amended) The security processing system of claim 33 [[47]] wherein the at least one ~~network~~ Ethernet controller securely communicates with the at least one security processor to configure the at least one security processor or retrieve status information from the at least one security processor.

57. (canceled).

58. (new) The method of claim 1, further comprising:

entering a low power state upon receipt of a low-power configuration signal, wherein entering the low power state includes:

disabling an IPSec data path and a public key data path.

59. (new) The method of claim 58, further comprising:

receiving a configuration signal indicating a release from low power state; and

enabling the IPSec data path and the public key data path.

60. (new) The method of claim 1, further comprising:

prior to receiving the internal outbound packet in a flow,
receiving security association information for the flow, the security association information including a security association handle and security association data.

61. (new) The method of claim 60, further comprising:

storing the security association information in a local memory associated with the security processor.

62. (new) The method of claim 1, wherein the security processor resides on a motherboard of a computer system.

63. (new) The security processor of claim 8, wherein the at least one processor is further configured to enter a low power state upon receipt of a low-power configuration signal and disable an IPSec data path and a public key data path.

64. (new) The security processor of claim 63, wherein the at least one processor is further configured to:

receive a configuration signal indicating a release from low power state; and

enable the IPSec data path and the public key data path.

65. (new) The security processor of claim 8, wherein the at least one processor is further configured to receive security association information for the flow, the security association information including a security association handle and security association data.

66. (new) The security processor of claim 65, wherein the at least one processor is further configured to store the security association information in a local memory associated with the security processor.

67. (new) The security processor of claim 8, wherein the security processor resides on a motherboard of a computer system.

68. (new) The security processor of claim 8, wherein the security processor is in-line with a data path of a packet network.